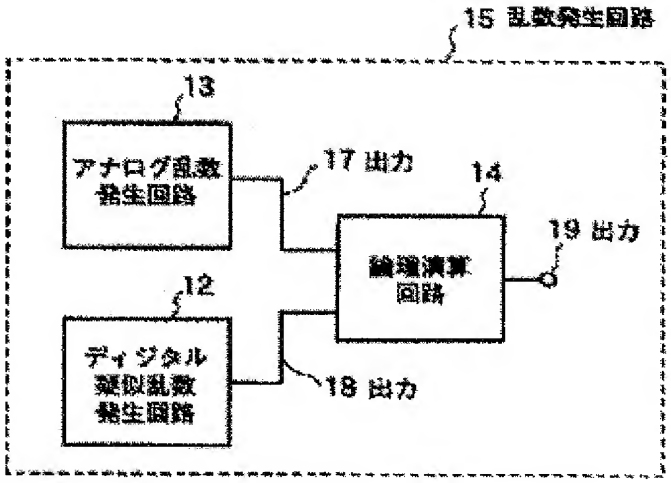
CIRCUIT FOR GENERATING RANDOM NUMBER

Publication number: JP2001344094
Publication date: 2001-12-14
Inventor: ISHII HARUHIKO; TANAKA YUKIO; KAMIYAMA KENICHI
Applicant: NTT ELECTRONICS CORP
Classification:
- international: ***G06F7/58; H03K3/84;*** **G06F7/58; H03K3/00;** (IPC1-7): G06F7/58; H03K3/84
- European:
Application number: JP20000163184 20000531
Priority number(s): JP20000163184 20000531

Abstract of **JP2001344094**

PROBLEM TO BE SOLVED: To realize a random number generating circuit in which the generation frequency of random numbers can be made uniform, and reproducibility can be prevented from being generated. SOLUTION: This circuit is provided with an analog random number generating circuit 13 for amplifying a noise generated like an analog from the fluctuation of currents running through electronic components such as a resistance or a semiconductor element, and for outputting it as random numbers, a digital pseudo random number generating circuit 12 for generating and outputting digital pseudo random numbers according to the combination of a register and a logical arithmetic element or a software arithmetic operation, and a logical arithmetic circuit 14 for performing the logical arithmetic operation of the output of the analog random number generating circuit 13 and the output of the digital pseudo random number generating circuit 12, and outputting the arithmetic result.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－344094
（P2001－344094A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ	５Ｊ０４９
Ｈ０３Ｋ　3/84		Ｈ０３Ｋ　3/84	Ｚ	

審査請求　有　　請求項の数２　ＯＬ　（全　４　頁）

(21)出願番号　特願2000－163184(P2000－163184)

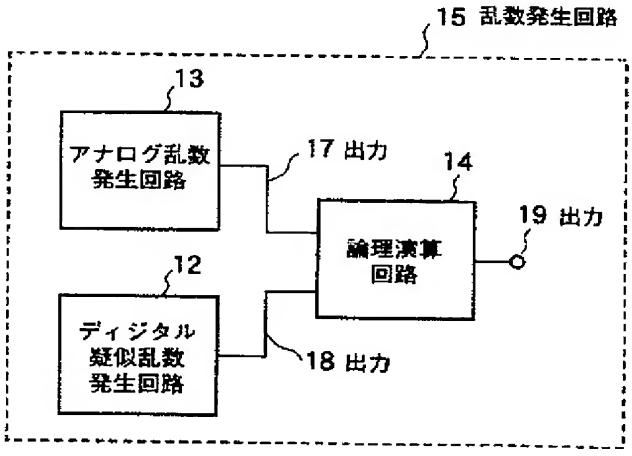
(22)出願日　平成12年５月31日(2000.5.31)

(71)出願人　591230295
エヌティティエレクトロニクス株式会社
東京都渋谷区道玄坂１丁目12番１号
(72)発明者　石井　春彦
東京都渋谷区道玄坂１－12－１　エヌティティエレクトロニクス株式会社内
(72)発明者　田中　幸男
東京都渋谷区道玄坂１－12－１　エヌティティエレクトロニクス株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　（外５名）

最終頁に続く

(54)【発明の名称】　乱数発生回路

(57)【要約】
【課題】本発明の課題は、発生頻度が一様でかつ再現性の無い乱数発生回路を簡易な構成で実現することにある。
【解決手段】本発明は、抵抗や半導体素子等の電子部品に流れる電流の揺らぎからアナログ的に発生する雑音を増幅して乱数として出力するアナログ乱数発生回路１３と、レジスタと論理演算素子の組合せあるいはソフトウエア演算によりディジタル疑似乱数を発生し出力するディジタル疑似乱数発生回路１２と、該アナログ乱数発生回路１３の出力と該ディジタル疑似乱数発生回路１２の出力とを論理演算して出力する論理演算回路１４とを具備することを特徴とするものである。



1

【特許請求の範囲】

【請求項１】　抵抗や半導体素子等の電子部品に流れる電流の揺らぎからアナログ的に発生する雑音を増幅して乱数として出力するアナログ乱数発生回路と、

レジスタと論理演算素子の組合せあるいはソフトウエア演算によりディジタル疑似乱数を発生し出力するディジタル疑似乱数発生回路と、

該アナログ乱数発生回路の出力と該ディジタル疑似乱数発生回路の出力とを論理演算して出力する論理演算回路とを具備することを特徴とする乱数発生回路。

【請求項２】　アナログ乱数発生回路として、相補形の２個のトランジスタペアの入力端子どうし及び出力端子どうしを接続したインバータと該インバータの入力端子と出力端子との間に接続された帰還抵抗とで構成されたインバータアンプをコンデンサを介在することにより複数段交流的に結合して初段のインバータアンプで発生したアナログ的雑音を増幅し乱数として出力するアナログ乱数発生回路を用いることを特徴とする請求項１記載の乱数発生回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は２値（１／０）の乱数を時系列的に発生させる乱数発生回路に関する。

【０００２】

【従来の技術】近年、クレジットカードなどで使用されている磁気カードの偽造防止対策として、暗号回路を搭載したＩＣカードの開発が進められている。セキュリティを高めるためには暗号回路内に発生頻度が一様でかつ再現性のない乱数を発生させる回路が必要である。

【０００３】従来、乱数（＝雑音）を発生させる方法としては、レジスタと論理回路の組合せにより疑似乱数を発生させる方法と、抵抗や半導体素子等に流れる電流の揺らぎに伴う雑音を増幅して２値乱数データを得る方法が多く用いられてきた。

【０００４】前者の代表例としてはM系列符号がある。図２は７段のM系列発生回路２１の構成例を示す。２２は７段のシフトレジスタであり、その４段目出力２３と７段目出力２４を入力とする排他的論理和回路（ＸＯＲ）２５の出力を１段目の入力に帰還しており、クロック２６の立上り毎に各段のシフトレジスタ２２のデータが右へ１ビットずつシフトされることにより、７段目の出力２４から２値の乱数が出力される。

【０００５】そのシリアル出力を７ビット毎に区切って数値化したデータ（１～１２７）の発生頻度は図３の乱数出力３１に示すように完全に均一化されており、偏りの無い理想的な乱数列を出力することができる。

【０００６】しかしながらこの方法では、アルゴリズムと初期値がわかると全く同じ乱数列が再現できるという大きな欠点があった。

【０００７】後者の例としては図４に示すようにツェナーダイオード４１に抵抗４２を介して電圧源４３から電流を流し、その両端に発生する雑音を増幅器４４で電源電圧まで増幅して出力４５に２値の雑音（＝乱数）を出力する方法がある。この方法では、電流の偶然の揺らぎを利用して雑音を発生するため、前者のように全く同じ雑音（＝乱数）が再現されるおそれは無いが、出力データの発生頻度は図５の乱数出力５１に示すように必ずしも均一なものが得られるとは限らず、出力されないデータ出力値も見られる。従来のこの方法では、精度の良い乱数を発生させることが困難という欠点があった。また、回路をＬＳＩ化する場合、通常多く使用されるＣＭＯＳプロセスではツェナーダイオードが容易に作成できないという欠点もあった。

2

【０００８】

【発明が解決しようとする課題】本発明は上記の事情に鑑みてなされたもので、発生頻度が一様で再現性の無い乱数を発生させる乱数発生回路を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するために本発明の乱数発生回路は、抵抗や半導体素子等の電子部品に流れる電流の揺らぎからアナログ的に発生する雑音を増幅して乱数として出力するアナログ乱数発生回路と、レジスタと論理演算素子の組合せあるいはソフトウエア演算によりディジタル疑似乱数を発生し出力するディジタル疑似乱数発生回路と、該アナログ乱数発生回路の出力と該ディジタル疑似乱数発生回路の出力とを論理演算して出力する論理演算回路とを具備することを特徴とするものである。

【００１０】また本発明は、前記乱数発生回路において、アナログ乱数発生回路として、相補形の２個のトランジスタペアの入力端子どうし及び出力端子どうしを接続したインバータと該インバータの入力端子と出力端子との間に接続された帰還抵抗とで構成されたインバータアンプをコンデンサを介在することにより複数段交流的に結合して初段のインバータアンプで発生したアナログ的雑音を増幅し乱数として出力するアナログ乱数発生回路を用いることを特徴とするものである。

【００１１】本発明による乱数発生回路は、ディジタル疑似乱数発生回路とアナログ乱数発生回路との出力どうしの論理演算をとることにより、上記の問題を解決するものである。

【００１２】即ち、均一性が不十分なアナログ的乱数を、再現されるおそれはあるが均一性の高いディジタル疑似乱数と論理演算することにより、スペクトラムを拡散し、再現性がなくかつ均一性が確保できる乱数を発生することを特徴とする。

【００１３】

【発明の実施の形態】以下図面を参照して本発明の実施形態例を詳細に説明する。

3

【００１４】本発明の一実施形態例を図１に示す。乱数発生回路１５はディジタル疑似乱数発生回路１２、アナログ乱数発生回路１３、及び論理演算回路１４より構成される。ディジタル疑似乱数発生回路１２は例えば図２に示すようなM系列符号等、ディジタル的に疑似乱数を発生させる回路であり、公知の技術で容易に実現できるものである。ディジタル疑似乱数発生回路１２の出力１８からは均一性の良いシリアル乱数データが出力される。アナログ乱数発生回路１３は電流の揺らぎ等、アナログ的な発生源から乱数（＝雑音）を発生させる回路であり、例えば図４に示すようなツェナーダイオードを利用した方法等の公知の従来技術でも実現できる。

【００１５】本発明による他の実施形態例としては、図６に示すようなインバータアンプを多段接続したアナログ乱数発生回路６０の構成によるものが使用可能である。

【００１６】６０３はインバータ素子であり、相補形の２個のトランジスタペアの入力端子どうし及び出力端子どうしを接続して構成される。例えばＣＭＯＳ－ＬＳＩプロセスではｎチャネルトランジスタとｐチャネルトランジスタ各１個の組合せで容易に実現できる。このインバータ素子６０３の入・出力端子間に抵抗６０４により負帰還をかけることにより、簡易な構成でアナログのインバータアンプ６１が実現できる。インバータアンプ６１の出力６０１には、内部トランジスタに流れる電流の揺らぎによる微小な雑音が発生し、コンデンサ６０２により交流的に結合された次段のインバータアンプ６１により増幅される。多段接続のインバータアンプ６１により電源電圧まで増幅された雑音振幅が出力バッファ回路６２により、２値のディジタル雑音信号に変換され、出力６３にシリアルで乱数として出力される。

【００１７】出力バッファ回路６２は通常ＣＭＯＳプロセスで多く用いられるディジタルインバータ素子等で容易に実現可能である。

【００１８】図１に示す乱数発生回路１５内の論理演算回路１４はアナログ乱数発生回路１３の出力１７とディジタル疑似乱数発生回路１２の出力１８を入力として論理演算を行い出力１９を生じる回路である。論理演算回路１４の簡単な例としては排他的論理和（ＸＯＲ）回路等が適用可能であるが、他のより複雑な論理回路であっても良い。

【００１９】論理演算回路１４により論理演算された乱数出力の発生頻度例を図７に示す。乱数出力７１は、図３のM系列符号と比較すると発生頻度には多少ばらつきが見られるものの、図５のアナログ乱数発生回路のような出力されないデータ出力値は見られず、大きな改善効果が見られる。

【００２０】

【発明の効果】以上説明したように本発明によれば、アナログ乱数発生回路により発生された再現性は無いが一様性が十分でない乱数と、ディジタル疑似乱数発生回路により発生された一様性は十分だが、再現性のある乱数とを論理演算することにより、両者の長所のみを取り出した一様性があり、再現性の無い乱数を容易に得ることができる。

4

【００２１】また、アナログ乱数発生回路については、インバータアンプを交流結合により複数段シリーズに接続することにより、ＬＳＩ化が容易になるという利点がある。

【００２２】なお、以上の説明ではディジタル疑似乱数発生回路は７段のM系列符号をハードウェアで発生する場合を例にとって説明したが、段数はこれ以外でもよく、また符号の種類もM系列以外のものでもよい。またマイクロプロセッサ等のソフトウエアで演算して実現する方法であってもよい。

【図面の簡単な説明】

【図１】本発明に係る乱数発生回路の一実施形態例を示す構成説明図である。

【図２】従来のディジタル疑似乱数発生回路の一例を示す回路図である。

【図３】図２のディジタル疑似乱数発生回路のデータ出力値に対する発生頻度の一例を示す特性図である。

【図４】従来のアナログ乱数発生回路の一例を示す回路図である。

【図５】図４のアナログ乱数発生回路のデータ出力値に対する発生頻度の一例を示す特性図である。

【図６】本発明に係るアナログ乱数発生回路の一例を示す回路図である。

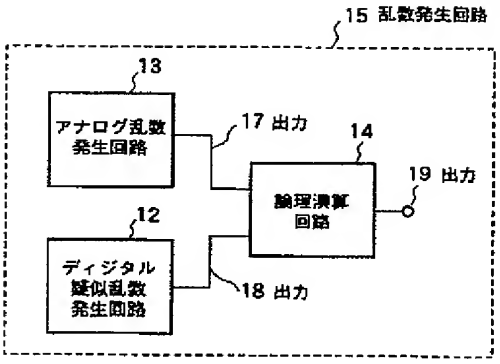
【図７】本発明に係る乱数発生回路のデータ出力値に対する発生頻度の一例を示す特性図である。

【符号の説明】

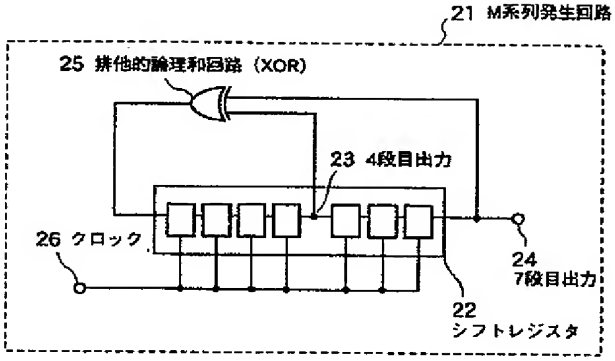
１２　ディジタル疑似乱数発生回路
１３，６０　アナログ乱数発生回路
１４　論理演算回路
１５　乱数発生回路
１７，１８，１９，４５，６３，６０１　出力
２１　M系列発生回路
２２　シフトレジスタ
２３　４段目出力
２４　７段目出力
２５　排他的論理和回路（ＸＯＲ）
２６　クロック
３１，５１，７１　乱数出力
４１　ツェナーダイオード
４２，６０４　抵抗
４３　電圧源
４４　増幅器
６１　インバータアンプ
６２　出力バッファ回路
６０２　コンデンサ

６０３　　インバータ素子

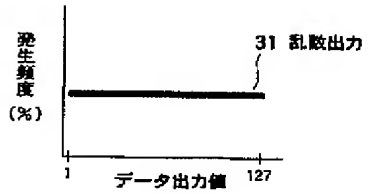
【図１】



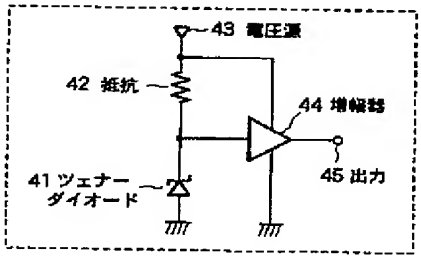
【図２】



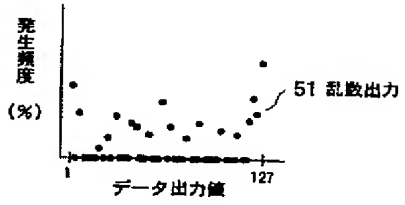
【図３】



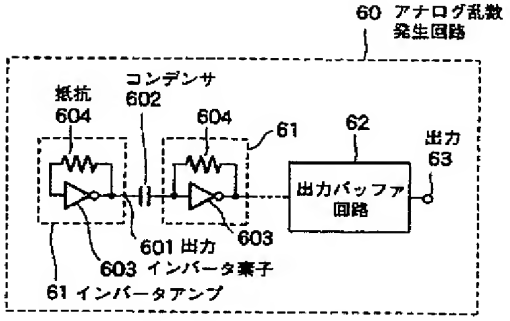
【図４】



【図５】



【図６】



【図７】

フロントページの続き

(72)発明者　神山　健一
東京都渋谷区道玄坂１－12－１　エヌティティエレクトロニクス株式会社内

Ｆターム(参考)　5J049 CA03 CA09 CA10